Secure Communication over Fading Channels with Statistical QoS Constraints

Deli Qiao, Mustafa Cenk Gursoy, and Senem Velipasalar
Department of Electrical Engineering
University of Nebraska-Lincoln, Lincoln, NE 68588
Email: dqiao726@huskers.unl.edu, gursoy@engr.unl.edu, velipasa@engr.unl.edu

***Abstract*—[1] In this paper, secure transmission of information over an ergodic fading channel is studied in the presence of statistical quality of service (QoS) constraints.We employ effective capacity to measure the secure throughput of the system, i.e., *effective secure throughput*. We assume that the channel side information (CSI) of the main channel is available at the transmitter side. Under different assumptions on the availability of the CSI of the eavesdropper channel, we investigate the optimal power control policies that maximize the *effective secure throughput*. In particular, when the CSI of the eavesdropper channel is available at the transmitter, it is noted that opportunistic transmission is no longer optimal and the transmitter should not wait to send the data at a high rate until the main channel is much better than the eavesdropper channel. Moreover, it is shown that the benefits of the CSI of the eavesdropper channel diminish as QoS constraints become more stringent.**

I. Introduction

Security is an important issue in wireless systems due to the broadcast nature of wireless transmissions. In a pioneering work, Wyner in [1] addressed the security problem from an information-theoretic point of view and considered a wire-tap channel model. He proved that secure transmission of confidential messages to a destination in the presence of a degraded wire-tapper can be achieved, and he established the secrecy capacity which is defined as the highest rate of reliable communication from the transmitter to the legitimate receiver while keeping the wire-tapper completely ignorant of the transmitted messages. Recently, there has been numerous studies addressing information theoretic security. For instance, the impact of fading has been investigated in [2], where it has been shown that a non-zero secrecy capacity can be achieved even when the eavesdropper channel is better than the main channel on average. The secrecy capacity region of the fading broadcast channel with confidential messages and associated optimal power control policies have been identified in [3], where it is shown that the transmitter allocates more power as the strength of the main channel increases with respect to that of the eavesdropper channel.

In addition to security issues, providing acceptable performance and quality is vital to many applications. For instance, voice over IP (VoIP) and interactive-video (e.g,. videoconferencing) systems are required to satisfy certain buffer or delay constraints. In this paper, we consider statistical QoS constraints in the form of limitations on the buffer length, and incorporate the concept of effective capacity [4], which can be seen as the maximum constant arrival rate that a given time-varying service process can support while satisfying statistical QoS guarantees. The analysis and application of effective capacity in various settings have attracted much interest recently (see e.g., [5]–[7] and references therein). We define the *effective secure throughput* as the maximum constant arrival rate that can be supported while keeping the eavesdropper ignorant of these messages in the presence of QoS constraints. We assume that the CSI of the main channel is available at the transmitter side. Then, we derive the optimal power control policies that maximize the effective secure throughput under different assumptions on the availability of the CSI of the eavesdropper channel. Through this analysis, we find that due to the introduction of QoS constraints, the transmitter cannot reserve its power for times at which the main channel is much stronger than the eavesdropper channel. Also, we note that the CSI of the eavesdropper provides little help when QoS constraints become more stringent.

The rest of the paper is organized as follows. Section II briefly describes the system model and the necessary preliminaries on statistical QoS constraints and effective capacity. In Section III, we present our results for both full and only main CSI scenarios. Finally, Section IV concludes the paper.

II. System Model and Preliminaries

A. System Model

The system model is shown in Fig. 1. It is assumed that the transmitter generates data sequences which are divided into frames of duration T. These data frames are initially stored in the buffer before they are transmitted over the wireless channel. The channel input-output relationships are given by

$$Y_1[i] = h_1[i]X[i] + Z_1[i] \tag{1}$$
$$Y_2[i] = h_2[i]X[i] + Z_2[i] \tag{2}$$

where i is the frame index, $X[i]$ is the channel input in the ith frame, and $Y_1[i]$ and $Y_2[i]$ represent the channel outputs at the receivers 1 and 2 in frame i, respectively. We assume that $\{h_j[i],\, j = 1,2\}$'s are jointly stationary and ergodic discrete-time processes, and we denote the magnitude-square

[1]This work was supported by the National Science Foundation under Grants CNS–0834753, and CCF–0917265.

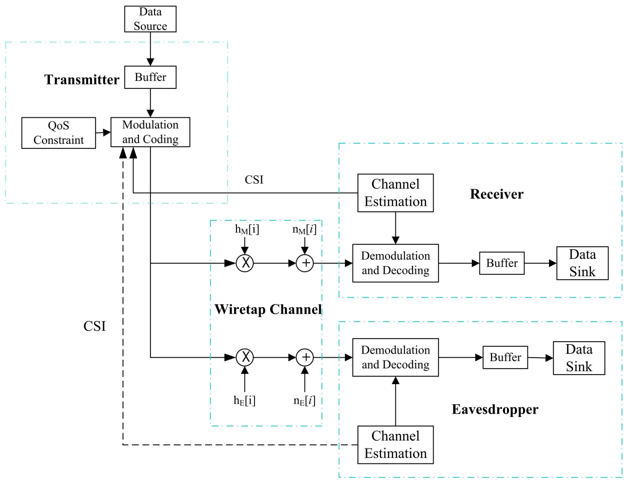

Fig. 1. The general system model.

of the fading coefficients by $z_j[i] = |h_j[i]|^2$. Considering that receiver 1 is the main user and receiver 2 is the eavesdropper, we in the rest of the paper express z_1 and z_2 as z_M and z_E, respectively, for more clarity. The channel input is subject to an average power constraint $\mathbb{E}\{|X[i]|^2\} \leq \bar{P}$, and we assume that the bandwidth available for the system is B. Above, the noise component $Z_j[i]$ is a zero-mean, circularly symmetric, complex Gaussian random variable with variance $\mathbb{E}\{|Z_j[i]|^2\} = N_j$ for $j = 1, 2$. The additive Gaussian noise samples $\{Z_j[i]\}$ are assumed to form an independent and identically distributed (i.i.d.) sequence.

We denote the average transmitted signal to noise ratio with respect to receiver 1 as $\text{SNR} = \frac{\bar{P}}{N_1 B}$. We also denote $P[i]$ as the instantaneous transmit power in the ith frame. Now, the instantaneous transmitted SNR level for receiver 1 can be expressed as $\mu^1[i] = \frac{P[i]}{N_1 B}$. Then, the average power constraint is equivalent to the average SNR constraint $\mathbb{E}\{\mu^1[i]\} \leq \text{SNR}$ for receiver 1. If we denote the ratio between the noise power of the two channels as $\gamma = \frac{N_1}{N_2}$, the instantaneous transmitted SNR level for receiver 2 becomes $\mu^2[i] = \gamma\mu^1[i]$.

B. Statistical QoS Constraints and Effective Secure Throughput

In [4], Wu and Negi defined the effective capacity as the maximum constant arrival rate[2] that a given service process can support in order to guarantee a statistical QoS requirement specified by the QoS exponent θ. If we define Q as the stationary queue length, then θ is the decay rate of the tail of the distribution of the queue length Q:

$$\lim_{q\to\infty} \frac{\log P(Q \geq q)}{q} = -\theta. \quad (3)$$

Therefore, for large $q_{\max}$, we have the following approximation for the buffer violation probability: $P(Q \geq q_{\max}) \approx e^{-\theta q_{\max}}$. Hence, while larger θ corresponds to more strict QoS constraints, smaller θ implies looser QoS guarantees. Similarly, if D denotes the steady-state delay experienced in the buffer, then $P(D \geq d_{\max}) \approx e^{-\theta\delta d_{\max}}$ for large $d_{\max}$, where δ is determined by the arrival and service processes [6].

The effective capacity is given by

$$C(\theta) = -\frac{\Lambda(-\theta)}{\theta} = -\lim_{t\to\infty} \frac{1}{\theta t} \log_e \mathbb{E}\{e^{-\theta S[t]}\} \quad \text{bits/s}, \quad (4)$$

where the expectation is with respect to $S[t] = \sum_{i=1}^{t} s[i]$, which is the time-accumulated service process. $\{s[i], i = 1, 2, \ldots\}$ denotes the discrete-time stationary and ergodic stochastic service process. We define the effective capacity obtained when the service rate is confined by the secrecy capacity as the *effective secure throughput*.

In this paper, in order to simplify the analysis while considering general fading distributions, we assume that the fading coefficients stay constant over the frame duration T and vary independently for each frame and each user. In this scenario, $s[i] = TR[i]$, where $R[i]$ is the instantaneous service rate for confidential messages in the ith frame duration $[iT, (i+1)T]$. Then, (4) can be written as

$$C(\theta) = -\frac{1}{\theta T} \log_e \mathbb{E}_{\mathbf{z}}\{e^{-\theta T R[i]}\} \quad \text{bits/s}, \quad (5)$$

where $R[i]$ in general depends on the fading magnitudes $\mathbf{z} = (z_M, z_E)$. (5) is obtained using the fact that instantaneous rates $\{R[i]\}$ vary independently over different frames. The *effective secure throughput* normalized by bandwidth B is

$$\mathsf{C}(\theta) = \frac{C(\theta)}{B} \quad \text{bits/s/Hz}. \quad (6)$$

III. Secrecy Capacity with QoS Constraints

Gopala *et al.* in [2] investigated the secrecy capacity in ergodic fading channels without delay constraints. They considered two cases: full CSI at the transmitter and only main CSI at the transmitter. In this section, we also consider these two cases but in the presence of statistical QoS constraints.

A. Full CSI at the Transmitter

In this part, we assume that the perfect CSI of the main channel and the eavesdropper channel is available at the transmitter. The transmitter is able to adapt the transmitted power according to the instantaneous values of z_M and z_E only when $z_M > \gamma z_E$. The secrecy capacity is then given by

$$R_s = \begin{cases} \log_2(1 + \mu(z_M, z_E) z_M) \\ -\log_2(1 + \gamma\mu(z_M, z_E) z_E), & z_M > \gamma z_E \\ 0, & \text{else.} \end{cases} \quad (7)$$

where $\mu(z_M, z_E)$ is the optimal power allocated when z_M and z_E are known at the transmitter.

In the presence of QoS constraints, the optimal power allocation policy in general depends on the QoS exponent θ[3].

[2]For time-varying arrival rates, effective capacity specifies the effective bandwidth of the arrival process that can be supported by the channel.

[3]Due to this dependence, we henceforth use $\mu(\theta, z_M, z_E)$ to denote the power allocation policy under QoS constraints.

Hence, the secure throughput can be expressed as

$$\mathsf{C}_E(\theta) = \max_{\substack{\mu(\theta,z_M,z_E)\\ \mathbb{E}\{\mu(\theta,z_M,z_E)\}\le \text{SNR}}} -\frac{1}{\theta TB}\log_e\left(\int_0^\infty\int_0^{z_E} p_{z_M}(z_M)p_{z_E}(z_E)dz_M dz_E + \int_0^\infty\int_{z_E}^\infty \left(\frac{1+\mu(\theta,z_M,z_E)z_M}{1+\gamma\mu(\theta,z_M,z_E)z_E}\right)^{-\beta} p_{z_M}(z_M)p_{z_E}(z_E)dz_M dz_E\right). \tag{8}$$

Note that the first term in the $\log$ function is a constant, and $\log$ is a monotonically increasing function. The maximization problem in (8) is equivalent to the following minimization problem

$$\min_{\substack{\mu(\theta,z_M,z_E)\\ \mathbb{E}\{\mu(\theta,z_M,z_E)\}\le \text{SNR}}} \int_0^\infty\int_{z_E}^\infty \left(\frac{1+\mu(\theta,z_M,z_E)z_M}{1+\gamma\mu(\theta,z_M,z_E)z_E}\right)^{-\beta} \times p_{z_M}(z_M)p_{z_E}(z_E)dz_M dz_E. \tag{9}$$

It is easy to check that when $z_M > \gamma z_E$

$$f(\mu) = \left(\frac{1+\mu z_M}{1+\gamma\mu z_E}\right)^{-\beta} \tag{10}$$

is a convex function in μ. According to [9], non-negative integral preserves convexity, hence the objective function is convex in μ. Then, we can form the following Lagrangian function, denoted as $\mathcal{J}$:

$$\mathcal{J} = \int_0^\infty\int_{z_E}^\infty \left(\frac{1+\mu(\theta,z_M,z_E)z_M}{1+\gamma\mu(\theta,z_M,z_E)z_E}\right)^{-\beta} p_{z_M}(z_M)p_{z_E}(z_E)dz_M dz_E + \lambda\left(\int_0^\infty\int_{z_E}^\infty \mu(\theta,z_M,z_E)p_{z_M}(z_M)p_{z_E}(z_E)dz_M dz_E - \text{SNR}\right) \tag{11}$$

Taking the derivative of the Lagrangian function over $\mu(\theta,z_M,z_E)$, we get the following optimality condition:

$$\frac{\partial\mathcal{J}}{\partial\mu(\theta,z_M,z_E)} = \lambda - \beta\left(\frac{1+\mu(\theta,z_M,z_E)z_M}{1+\gamma\mu(\theta,z_M,z_E)z_E}\right)^{-\beta} \times \frac{z_M-\gamma z_E}{(1+\mu(\theta,z_M,z_E)z_M)(1+\gamma\mu(\theta,z_M,z_E)z_E)} = 0 \tag{12}$$

where λ is the Lagrange multiplier whose value is chosen to satisfy the average power constraint with equality. For any channel state pairs (z_M, z_E), $\mu(\theta,z_M,z_E)$ can be obtained from the above condition. Whenever the value of $\mu(\theta,z_M,z_E)$ is negative, it follows from the convexity of the objective function with respect to $\mu(\theta,z_M,z_E)$ that the optimal value of $\mu(\theta,z_M,z_E)$ is 0.

There is no closed-form solution to (12). However, since the left-hand side of (12) is a monotonically increasing concave function, numerical techniques such as bisection search method can be efficiently adopted to derive the solution.

The secure throughput can be determined by substituting the optimal power control policy for $\mu(\theta,z_M,z_E)$ in (8). Exploiting the optimality condition in (12), we can notice that when $\mu(\theta,z_M,z_E)=0$, we have $z_M-\gamma z_E=\frac{\lambda}{\beta}$. Meanwhile,

$$\left(\frac{1+\mu(\theta,z_M,z_E)z_M}{1+\gamma\mu(\theta,z_M,z_E)z_E}\right)^{-\beta} \times \frac{1}{(1+\mu(\theta,z_M,z_E)z_M)(1+\gamma\mu(\theta,z_M,z_E)z_E)} < 1. \tag{13}$$

Thus, we must have $z_M-\gamma z_E > \frac{\lambda}{\beta}$ for $\mu(\theta,z_M,z_E)>0$, i.e., $\mu(\theta,z_M,z_E)=0$ if $z_M-\gamma z_E\le\frac{\lambda}{\beta}$. Hence, we can write the secure throughput as

$$\mathsf{C}_E(\theta) = -\frac{1}{\theta TB}\log_e\left(\int_0^\infty\int_0^{\gamma z_E+\frac{\lambda}{\beta}} p_{z_M}(z_M)p_{z_E}(z_E)dz_M dz_E + \int_0^\infty\int_{\gamma z_E+\frac{\lambda}{\beta}}^\infty \left(\frac{1+\mu(\theta,z_M,z_E)z_M}{1+\gamma\mu(\theta,z_M,z_E)z_E}\right)^{-\beta} \times p_{z_M}(z_M)p_{z_E}(z_E)dz_M dz_E\right) \tag{14}$$

where $\mu(\theta,z_M,z_E)$ is the derived optimal power control policy.

B. Only Main Channel CSI at the Transmitter

In this section, we assume that the transmitter has only the CSI of the main channel (the channel between the transmitter and the legitimate receiver). Under this assumption, it is shown in [2] that the secrecy rate for a specific channel state pair becomes

$$R_s = [\log_2(1+\mu(z_M)z_M) - \log_2(1+\gamma\mu(z_M)z_E)]^+ \tag{15}$$

where $\mu(z_M)$ is the optimal power allocated when only z_M is known at the transmitter.

In this case, the secure throughput can be expressed as

$$\mathsf{C}_E(\theta) = \max_{\substack{\mu(\theta,z_M)\\ \mathbb{E}\{\mu(\theta,z_M)\}\le \text{SNR}}} -\frac{1}{\theta TB}\log_e\left(\int_0^\infty\int_{z_M}^\infty p_{z_M}(z_M)p_{z_E}(z_E)dz_E dz_M + \int_0^\infty\int_0^{z_M} \left(\frac{1+\mu(\theta,z_M)z_M}{1+\gamma\mu(\theta,z_M)z_E}\right)^{-\beta} p_{z_M}(z_M)p_{z_E}(z_E)dz_E dz_M\right). \tag{16}$$

Similar to the discussion in Section III-A, we get the following equivalent minimization problem:

$$\min_{\substack{\mu(\theta,z_M)\\ \mathbb{E}\{\mu(\theta,z_M)\}\le \text{SNR}}} \int_0^\infty\int_0^{z_M} \left(\frac{1+\mu(\theta,z_M)z_M}{1+\gamma\mu(\theta,z_M)z_E}\right)^{-\beta} \times p_{z_M}(z_M)p_{z_E}(z_E)dz_M dz_E. \tag{17}$$

The objective function in this case is convex, and with a similar Lagrangian optimization method, we can get the following

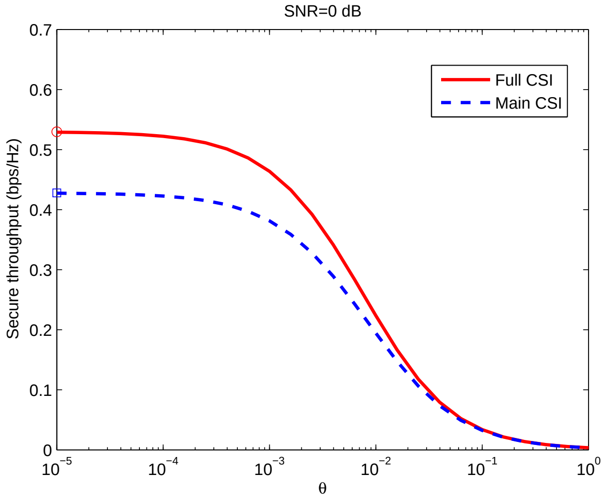

Fig. 2. The effective secure throughput with θ in Rayleigh channel with $\mathbb{E}\{z_E\} = \mathbb{E}\{z_M\} = 1$. $\gamma = 1$.

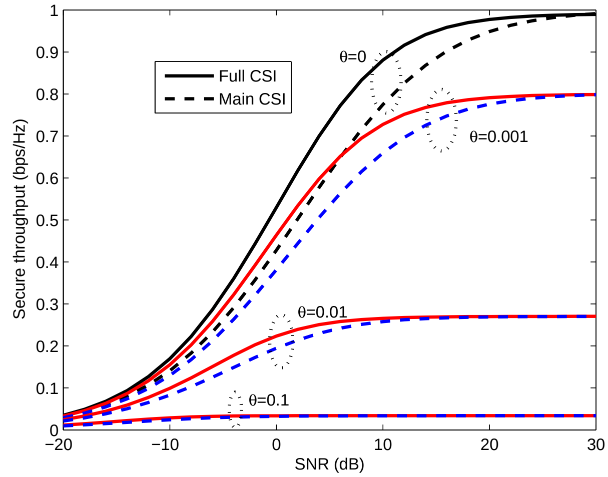

Fig. 3. The effective secure throughput with SNR in Rayleigh channel with $\mathbb{E}\{z_E\} = \mathbb{E}\{z_M\} = 1$. $\gamma = 1$.

optimality condition:

$$\frac{\partial \mathcal{J}}{\partial \mu(\theta, z_M)} = -\beta \int_0^{z_M} \left(\frac{1 + \mu(\theta, z_M) z_M}{1 + \gamma \mu(\theta, z_M) z_E} \right)^{-\beta - 1} \times \frac{z_M - \gamma z_E}{(1 + \gamma \mu(\theta, z_M) z_E)^2} p_{z_E}(z_E) dz_E + \lambda = 0 \tag{18}$$

where λ is a constant chosen to satisfy the average power constraint with equality. If the obtained power level $\mu(\theta, z_M)$ is negative, then the optimal value of $\mu(\theta, z_M)$ becomes 0 according to the convexity of the objective function in (17). Now that non-negative integral does not change the concavity, the LHS of (18) is still a monotonic increasing concave function of $\mu(\theta, z_M)$.

The secure throughput can be determined by substituting the optimal power control policy for $\mu(\theta, z_M)$ in (16). Exploiting the optimality condition in (18), we can notice that when $\mu(\theta, z_M, z_E) = 0$, we have

$$-\beta \int_0^{z_M} (z_M - \gamma z_E) p_{z_E}(z_E) dz_E + \lambda = 0 \tag{19}$$

$$\Rightarrow \int_0^{z_M} P(z_E \leq t) dt = \frac{\lambda}{\beta} \tag{20}$$

Denote the solution to the above equation as α. Considering that

$$\left(\frac{1 + \mu(\theta, z_M, z_E) z_M}{1 + \gamma \mu(\theta, z_M, z_E) z_E} \right)^{-\beta - 1} \frac{1}{(1 + \gamma \mu(\theta, z_M, z_E) z_E)^2} < 1, \tag{21}$$

we must have $z_M > \alpha$ for $\mu(\theta, z_M) > 0$, i.e., $\mu(\theta, z_M) = 0$ if $z_M \leq \alpha$. Hence, we can write the secure throughput as

$$\mathsf{C}_E(\theta) = -\frac{1}{\theta T B} \log_e \left(\int_0^{\alpha} \int_0^{\infty} p_{z_M}(z_M) p_{z_E}(z_E) dz_E dz_M + \int_{\alpha}^{\infty} \int_{z_M}^{\infty} p_{z_M}(z_M) p_{z_E}(z_E) dz_E dz_M + \int_{\alpha}^{\infty} \int_0^{z_M} \left(\frac{1 + \mu(\theta, z_M) z_M}{1 + \gamma \mu(\theta, z_M) z_E} \right)^{-\beta} \tag{22}$$

$$\times p_{z_M}(z_M) p_{z_E}(z_E) dz_E dz_M \right) \tag{23}$$

where $\mu(\theta, z_M)$ is the derived optimal power control policy.

C. Numerical Results

In Fig. 2, we plot the effective secure throughput as a function of the QoS exponent θ in Rayleigh fading channel with $\gamma = 1$ for the full and main CSI scenarios. It can be seen from the figure that as the QoS constraints become more stringent and hence as the value of θ increases, little help is provided by the CSI of the eavesdropper channel. In Fig. 3, we plot the effective secure throughput as SNR varies for $\theta = \{0, 0.001, 0.01, 0.1\}$. Not surprisingly, we observe that the availability of the CSI of the eavesdropper channel at the transmitter does not provide much gains in terms of increasing the effective secure throughput in the large SNR regime. Also, as QoS constraints becomes more strict, we similarly note that having the CSI of the eavesdropper channel does not increase the rate of secure transmission much even at medium SNR levels.

To have an idea of the power allocation policy, we plot the power distribution as a function of (z_E, z_M) for full CSI case when $\theta = 0.01$ and $\theta = 0$ in Fig. 4. In the figure, we see that for both values of θ, no power is allocated for transmission when $z_M < z_E$ which is expected under the assumption

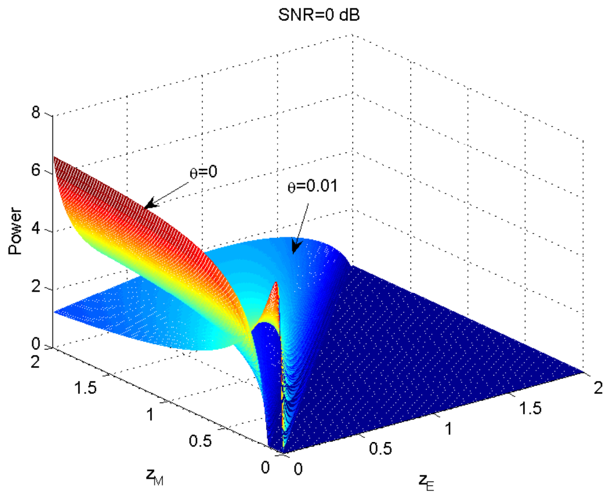

Fig. 4. The power allocation for full CSI scenario with SNR $= 0$ dB in Rayleigh channel with $\mathbb{E}\{z_E\} = \mathbb{E}\{z_M\} = 1$. $\gamma = 1$.

of equal noise powers, i.e., $N_1 = N_2$. We note that when $\theta = 0$ and hence there are no buffer constraints, opportunistic transmission policy is employed. More power is allocated for cases in which the difference $z_M - z_E$ is large. Therefore, the transmitter favors the times at which the main channel is much better than the eavesdropper channel. At these times, the transmitter sends the information at a high rate with large power. When $z_M - z_E$ is small, transmission occurs at a small rate with small power. However, this strategy is clearly not optimal in the presence of buffer constraints because waiting to transmit at high rate until the main channel becomes much stronger than the eavesdropper channel can lead to buildup in the buffer and incur large delays. Hence, we do not observe this opportunistic transmission strategy when $\theta = 0.01$. In this case, we note that a more uniform power allocation is preferred. In order not to violate the limitations on the buffer length, transmission at a moderate power level is performed even when $z_M - z_E$ is small.

IV. Conclusion

In this paper, we have anayzed the secrecy capacity in the presence of statistical QoS constraints. We have considered the *effective secure throughput* as a measure of the performance. With different assumptions on the availability of the full and main CSI at the transmitter, we have investigated the associated optimal power allocation policies that maximize the effective secure throughput. In particular, we have noted that the transmitter allocates power more uniformly instead of concentrating its power for the cases in which the main channel is much stronger than the eavesdropper channel. By numerically comparing the obtained effective secure throughput, we have shown that as QoS constraints become more stringent, the benefit of having the CSI of the eavesdropper channel at the transmitter diminishes.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, Oct. 1975.

[2] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theo.*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels,"*IEEE Trans. Inform. Theory*, vol. 54, pp. 2470-2492, June 2008.

[4] D. Wu and R. Negi "Effective capacity: a wireless link model for support of quality of service," *IEEE Trans. Wireless Commun.*, vol.2,no. 4, pp.630-643. July 2003

[5] J. Tang and X. Zhang, "Quality-of-service driven power and rate adaptation over wireless links," *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 3058-3068, Aug. 2007.

[6] J. Tang and X. Zhang, "Cross-layer-model based adaptive resource allocation for statistical QoS guarantees in mobile wireless networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp.2318-2328, June 2008.

[7] L. Liu, P. Parag, and J.-F. Chamberland, "Quality of service analysis for wireless user-cooperation networks," *IEEE Trans. Inform. Theory*, vol. 53, no. 10, pp. 3833-3842, Oct. 2007

[8] A. Goldsmith, *Wireless Communications*, 1st ed. Cambridge University Press, 2005.

[9] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.